UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with "Kevin Brown; 531-215-2341" that is stored at premises controlled by Apple, Inc.

See Attachment A

Case No. 4:18MJ3120

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Information associated with "Kevin Brown; 531-215-2341" that is stored at premises controlled by Apple, Inc.

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2113	Bank Robbery

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brandon Day, S.A., FBI
Printed name and title

- ☒ Sworn to before me and signed in my presence.
- ☐ Sworn to before me by telephone or other reliable electronic means.

Date: 08/20/2018

Judge's signature

City and state: Lincoln, Nebraska

CHERYL R. ZWART, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEBRASKA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH "**KEVIN BROWN; 531-215-2341**" THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case No. 4:18MJ3120

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brandon Day, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed account (Apple ID) that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I have been a Special Agent of the Federal Bureau of Investigation (FBI) since March 2016. Prior to that, I was a Special Agent with the Drug Enforcement Administration (DEA) in St. Louis, Missouri, and a police officer with the Lincoln Police Department in Lincoln, Nebraska. I have participated in numerous and varied criminal

investigations, from robbery investigations to drug trafficking investigations. I have authored numerous affidavits in support of search warrants for physical locations, various electronic devices as well as service provider accounts**.**

3. The facts in this affidavit come from my personal observations, my training and experience, and information and reports obtained from other agents, investigators, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of bank robbery, 18 U.S.C. § 2113(a), has been committed by Kevin Lee Brown, and co-conspirators. There is also probable cause to believe Attachment A contains evidence of the crime, and other evidence of violations of 18 U.S.C. § 2113(a), as described in Attachment B.

PROBABLE CAUSE

5. On June 22, 2018, at approximately 8:38 a.m., two males pulled in front of the Great Western Bank, 8380 Old Cheney Road #1, Lincoln, Nebraska in a gold Hyundai Elantra, Nebraska license plate VGE626. Two males exited the vehicle and entered into the bank. One of the males had a flesh colored mask and sunglasses covering his face, was wearing a red hooded sweatshirt, jeans, sunglasses, white gloves, and a camouflage colored bandana on his head. The male kept one hand inside the sweatshirt pocket during the robbery. Although no weapon was seen, employees believed that he may have had a gun in that hand. The second suspect was wearing a blue medical mask and had on a long black wig, a white sweatshirt, dark pants, gloves, and was carrying a red duffle bag.

6. The males told the bank employees to put their hands up and lie on the ground. The first male walked around the bank and remained in the lobby with the employees. The second male told employees to give him the money. This male emptied the currency of two drawers into the red duffle bag and told two employees to open the bank vault. He then placed cash from the vault into the red duffle bag. A review of the bank video surveillance shows a white vehicle, a Jeep Grand Cherokee, driving through and stopping in the ATM lane of the parking lot seconds after the gold Hyundai arrived in front of the bank. The video surveillance shows the two suspects who robbed the bank exiting the gold Hyundai and entering the bank. These subjects are shown on surveillance video to exit the bank and depart the parking lot in the gold Hyundai at approximately 8:42 a.m.

7. A witness, who I will identify as "DH," reported observing the gold Hyundai and a white Jeep arrive together and park along the curb of Betty Lou Boulevard, between Glyn Oaks Drive and Lea Rae Drive in Lincoln, Nebraska, approximately 2-3 blocks from Great Western Bank, 8380 Old Cheney Road #1, Lincoln, Nebraska. DH observed the front seat passenger, carrying a red duffle bag, exit the Hyundai and enter into the passenger side of the white Jeep and depart in the Jeep at a high rate of speed. Due to DH's vantage point there was no view of the driver of either vehicle. The Hyundai remained in place until it was seized by Lincoln Police Department (LPD) officers.

8. At approximately 9:05 a.m., Deputy Schmuecker of the Lancaster County Sherriff's Office (LCSO) observed a white Jeep, Nebraska license plate VVD592, travel eastbound on Highway 6 at approximately 98th Street in Lincoln, Nebraska. The vehicle drew his attention because it was tailgating another vehicle and was very clean, which indicated to him that it was a rental vehicle. Deputy Schmuecker observed that the driver was a black male with facial hair,

estimated to be in his 30's. Deputy Schmuecker believed he saw a piece of red clothing on the driver but could not specify what article of clothing. Deputy Schmuecker only saw the driver of the vehicle and did not observe any other vehicle occupants. Deputy Schmuecker recorded the Jeep's plate over the dispatch radio. After losing sight of the vehicle the suspect vehicle description was updated to reflect that a white Jeep was involved in the bank robbery.

9. I updated Omaha FBI Special Agent (SA) John Hallock with the suspect vehicle information and he conducted a query of the 2018 White Jeep Grand Cherokee, Nebraska License VVD592. The query determined that the vehicle was registered to Easy Car Rent a Company, DBA Budget Rent A Car of Nebraska, 1755 East Locust Street, Omaha, Nebraska68110. SA Hallock made contact with a representative at Easy Car Rent a Company, who reported that the vehicle had been rented to a black male identified as Kevin Lee Brown, born in 1987. The representative reported that the vehicle was rented to Brown on June 18, 2018, and was due back on June 21, 2018.

10. On June 22, 2018, the representative from Easy Rent a Car Company contacted SA Hallock and reported that Brown had arrived at the company with the 2018 White Jeep Cherokee and wanted to exchange it for another vehicle. SA Hallock contacted members of the FBI Omaha Division Great Plains Violent Crime Task Force, who were in the immediate area. The task force members made contact with Brown, detained him, and explained that they were conducting a bank robbery investigation. Members of the task force located a white garbage bag sitting next to Brown when he was at customer service counter. The bag, without looking inside, appeared to contain red and blue clothing. Members of the task force reported that one of the employees at Easy Rent a Car Company saw Brown carry the white garbage bag inside the business with him. A subsequent review of the store's video surveillance shows Brown enter the store carrying the white bag before

setting it on the ground next to the counter. Members of the task force patted down Brown for weapons and contraband with negative findings, and waited for a police cruiser to respond in order to transport Brown to the Omaha Police Department (OPD) for purposes of an interview. Members of the task force transported the white garbage bag which contained the clothing to OPD for safekeeping.

11. A review of store video surveillance shows Brown holding, and appear to be using, his cell phone for several minutes before task officers arrived. Upon arriving, Brown is detained and his cell phone is secured by a task force member. OPD Task Force Officer Jon Martin, assigned to the FBI Omaha Division Great Plains Violent Crime Task Force, seized the silver IPhone as evidence. TFO Martin reported that an ATM card and a driver's license that belonged to Brown were with the phone. Telephone number 531-215-2341 was listed as Brown's telephone number in the car rental paperwork.

12. On June 22, 2018, at OPD, SA Hallock and TFO Martin attempted to interview Brown. Brown was read his Miranda rights, and immediately invoked his Miranda rights, stating he wanted to speak to an attorney. The interview was immediately terminated.

13. On June 22, 2018, in the United States District Court, District of Nebraska, the Honorable Susan M. Bazis, United States Magistrate Judge, signed a search warrant for the search of the white garbage bag and search warrant for the 2018 White Jeep Grand Cherokee with Nebraska License VVD592. Oh that same day task force officers assigned to the FBI Omaha Division Great Plains Violent Crime Task Force searched the white garbage bag, which produced a Caucasian male flesh type mask, a camouflage colored bandana, and a pair of white gloves. A review of the video surveillance from Great Western Bank determined that one of the robbers was wearing a Caucasian flesh type mask, a camouflage colored bandana, and a pair of white gloves.

14. On June 7, 2018 a search of the white 2018 Jeep Grand Cherokee was conducted at the Omaha Police Department (OPD) impound lot, located at 7809 F Street, Omaha, Nebraska. The search of the vehicle produced a Hyundai car key found under the back passenger seat of the vehicle, and a rental agreement contract for Kevin Lee Brown, with a last known address of 1847 North 17th Street, Omaha, Nebraska, for the 2018 white Jeep Grand Cherokee.

15. On June 28, 2018, in the United States District Court, District of Nebraska, the Honorable Susan M. Bazis, United States Magistrate Judge, signed a search warrant for the Silver IPhone 6 that was in Brown's possession upon his arrest. A download of the phone was attempted. The phone is currently in "locked" status and due to security features of this generation of IPhone, FBI specialists advised that a download of the phone without the security code would take several years. As a result a download and subsequent search of the phone did not occur.

16. **INFORMATION REGARDING APPLE ID AND iCLOUD**[1]

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain

enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. Apple is able to determine a specific Apple ID based upon a user's full name and telephone number.

20. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address

(often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

21. Apple captures information associated with the creation and use of a Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

22. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email

account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

23. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

24. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and

videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

25. Based on my training and experience, and my conversations with other investigators knowledgeable of this matter, users of Apple devices frequently upload and/or store data to their iCloud account(s). Knowledge of the full contents of Brown's iCloud account, information connected to Brown's Apple ID, and other related records maintained by Apple, may provide significant information to assist in locating Brown's co-conspirators and provide evidence of violations of 18 U.S.C. § 2113(a). This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

26. Based on my training and experience, users of Apple iPhone devices are prompted to create an Apple ID as well as an iCloud account. Instant messages, emails, voicemails, photographs, videos, and documents are often created and uploaded to a user's iCloud account. These communications and photographs may provide vital clues regarding Brown's co-conspirators. Additionally, because much of the data located in a user's iCloud account and/or information connected to a user's Apple ID is tagged with a specific date, time,

and/or geo-location information, such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Specifically Brown's physical whereabouts between the time of the robbery and his contact with law enforcement officials upon returning the rental vehicle.

27. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services and/or mobile applications used to communicate with possible co-conspirators. Likewise emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of perpetrators and/or their co-conspirators and instrumentalities of the crimes under investigation.

28. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning Brown and his use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant.

31. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Brandon Day
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 20, 2018

CHERYL R. ZWART
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with user **KEVIN BROWN,** telephone number **(531) 215-2341** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2113(a), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

c. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with "Kevin Brown; 531-215-2341" that is stored at premises controlled by Apple, Inc.	)	Case No. 4:18MJ3120

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

Information associated with "Kevin Brown; 531-215-2341" that is stored at premises controlled by Apple, Inc.

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before September 4, 2018 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to CHERYL R. ZWART .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: **2:00 PM, Aug 20, 2018**

Judge's signature

City and state: Lincoln, Nebraska

CHERYL R. ZWART, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 4:18MJ3120	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with user **KEVIN BROWN,** telephone number **(531) 215-2341** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2113(a), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

c. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.